BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

デジタルコミュニケーションの総合誌

INTERNET magazine

1998年4月1日発行(毎月1日発行)通巻第39号

IP
We Love Internet-People
6Mbps No.39
【インターネットマガジン】
定価980円

【緊急企画】最新インターネット機能満載
これがウィンドウズ98だ!!

【集中企画】OCNユーザー必読
FreeBSDで最強の
インターネットサーバーを作ろう!!

【レポート】あの興奮はこうして伝えられた
長野はネットでオリンピック

【新連載】いつでもどこでもインターネット
走ろう!ニバイル道

【ハンズオン】「いま」が共有できる便利ツール
話題のICQを使ってみよう

【好評連載中】
インターネットでの不正行為~その傾向と対策
インターネット最新テクノロジー「VPN」
[illegible]

【インターネットde□□ページ】
[illegible]「□□□□□人」
[illegible]が選んだミステリーサイト
[illegible]から選んだツールサイト10

【詳細入門ページ】Win & Mac
まだつないでいない人のための
インターネット接続マニュアル

【業界でもっとも信頼できるデータ集】
掲載プロバイダー802社(↑13/↓2)
●料金一覧 ●話中度調査 ●相互接続マップ
●CD-ROMで一発検索:プロバイダーショックドサーチ(Win/Mac)

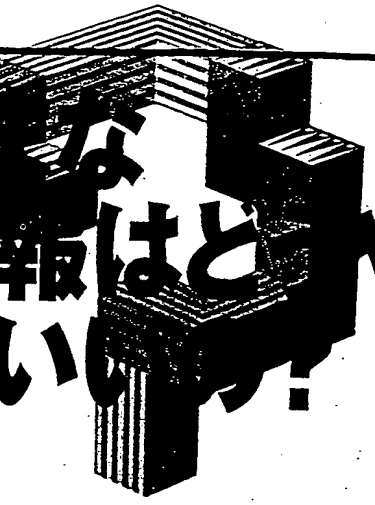
PRESENT & MONITOR
最新PHS対応PCやFreeBSDなど
プレゼント&商品モニター大募集!

定番ソフトから便利ツールまで、すべてそろうフリー&シェアウェア300本以上収録
CD-ROM

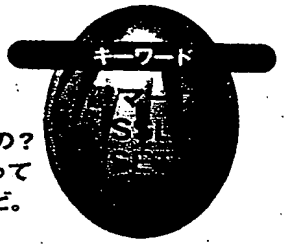
Internet Basics

【特集】忙しい人でも30分でわかる
いま答える!インターネットの大疑問

さまざまな個人情報はどうやって守ればいい？



**インターネットでは
フリーソフトの登録や
ショッピングなどで
個人情報を送信する
ことがあるけど
誰かに見られる危険はないの？
クレジットカードは危ないって
雑誌に書いてあったんだけど。**



石川和也
（伊藤忠テクノサイエンス㈱）

「鍵のマーク」は安心の印

インターネットでオンラインショッピングを利用する人が増えている。それにともなってセキュリティーやプライバシーといったことがますます注目されてきている。問題点も挙げられている。では、現実にはプライバシー、つまり個人情報の漏洩や盗難に対して何か対策が用意されているのだろう。もちろん、ユーザーが安心してインターネットを利用するためのセキュリティーシステムはいくつかある。

そのなかでもっともポピュラーなのが、ブラウザーの「鍵」マークだ。ネットスケープのナビゲーターでもマイクロソフトのインターネットエクスプローラでも、オンラインショッピングができるウェブページにアクセスしたときに、ウィンドウの下部の「鍵」のマークが、開いている状態から施錠された状態に変わることがある（鍵のグラフィックと位置は、ブラウザーとバージョンによって異なる。インターネットエクスプローラは通常は表示されていない）。実はこの鍵マークが1つの安心の目安といえるのだ。

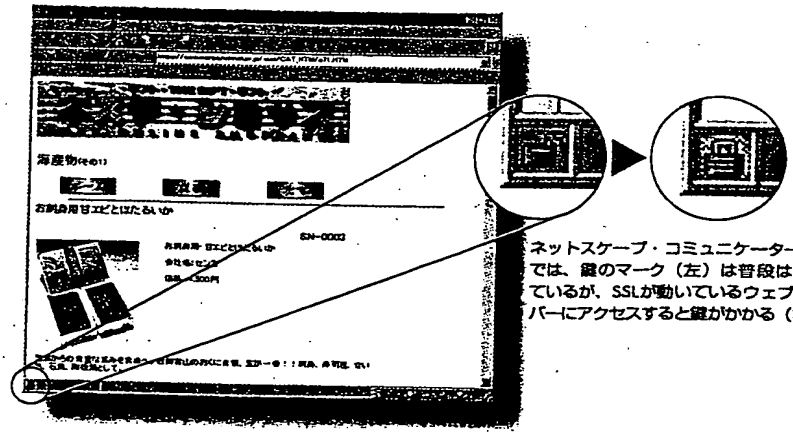
この鍵がかかるということは、クライアントマシン（ユーザー）とウェブサーバーとの通信が暗号化されてやり取りされるということを示している。つまりこの状態になると、クレジットカードの番号を入力して送信しても、他人にそれをのぞかれる心配が少なくなるわけだ。さらに、そのクレジットカード番号を送った先のショッピングサイトが誰なのか、本当にそのショッピングサイトの運営者であるかどうかを識別するためのウェブサイトの証明書が添付される（図）。ブラウザーの鍵マークをクリックして証明書を見ることにより、誰かがそのショッピングサイトになりすましていないかを確認することができる。同時に、もしここでショッピングをしたときに、商品を1つしか注文していないのに、10個も注文したかのように購入データが書き換えられることも防止できるのだ。このように、鍵がかかったウェブサイトでは、より安全なショッピングが行える。オンラインショッピングをするなら、鍵のかかったショッピングサイトで。これがもっとも簡単に、ユーザー側でできるセキュリティー対策だ。

鍵マークの正体はSSLだ

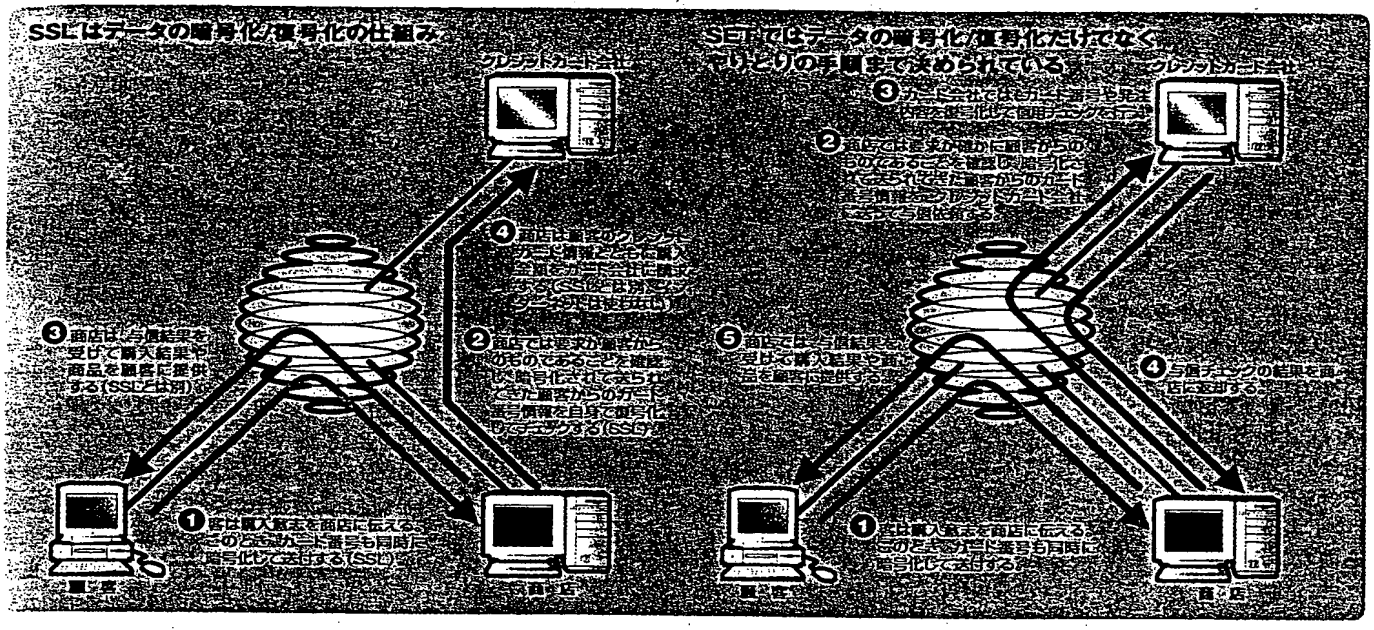
これらは、SSL（Secure Sockets Layer）と呼ばれる技術を使っている。SSLはネットスケープ社によって開発され、同社のブラウザー（ナビゲーター）やサーバー群（スイートスポット）をはじめ、インターネットエクスプローラでも利用可能なために、現在では業界標準となっている。

SSLは通信中のある一部のデータだけを暗号化するのではなく、TCP/IPで通信される内容をすべて暗号化する。SSLはアプリケーションとTCP/IPの中間に位置しており、アプリケーションから送られるデータを暗号化してTCP/IPのプロトコルに送り出し、また逆に外部から受け取った暗号化されたデータを復号してアプリケーションに渡している。つまりデータがコンピュータから外に出たときにはすでに暗号化されているわけだ。

このように、アプリケーション側ではデータの暗号化/復号化を意識する必要がない。しかも、TCP/IPで動作するアプリケーションならウェブ以外でも利用することができる。またSSLでは、通信に先立って電子証明書を確認することで相手を認証しているので、なりすましや改ざんを防げる。



ネットスケープ・コミュニケーター4.0では、鍵のマーク（左）は普段は開いているが、SSLが動いているウェブサーバーにアクセスすると鍵がかかる（右）。

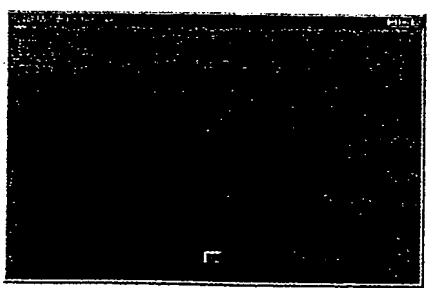


というわけで、ブラウザーの「鍵がかかる」ということは、SSLがオンになり、データを暗号化してやりとりします、ということなのだ。

SSLも万能ではない

それでは、SSLでサーバーが運用されていればそれでまったく問題はないのか。

SSLでは暗号化の方式としてさまざまな方式を利用できるように設計されており、米国内では鍵の長さ（暗号の強さを示す指標の1つ）が128ビットまで利用できる。しかし米国政府の輸出規制により、日本では40ビットに制限されている。たとえば、米国ネットスケープ社のホームページからダウンロードするナビゲーターも、使用地域選択で「JAPAN」を選ぶと、40ビット版がダウンロードされる。もちろん、パッケージ版や雑誌の付録CD-ROMに入っているのものも同様だ。



鍵マークをクリックすると証明書を見ることができる。

このレベル（40ビット）では、計算上はPentium（200MHz）を搭載したパソコンを利用すると約2か月半で1つのメッセージを解読することができるといわれている。また、SSLはネットワーク上の通信を暗号化するために設計されているため、アプリケーション側では、データは暗号化もされずにそのまま利用される。つまり、ウェブサーバーが受け取ったクレジットカード番号は複号化されて扱われるために、そのシステムが外部からアクセス可能な環境であれば、盗み出される危険があるということだ。そのため、ほとんどのクレジットカード会社ではショッピングサイトがインターネットでクレジットカードによる決済を行う場合には、カード情報などを暗号化してデータベースに保存することや、サイト自身をファイアーウォールなどで外部と遮断することなどを最低条件としているようだ。

SETによるクレジット決済

このようなSSLの問題点を解決するために、クレジットカード会社が中心となって進めている規格にSET（Secure Electronic Transaction）というものがある。SETは暗号化やなりすまし、改ざん防止ではSSLと同様の公開鍵（電子証明書）を利用しており、また暗号化/復号化だけではなく、クライアントとサーバー、そしてクレジットカード会社（など）とのデータのやりとりの手順までを定めたものだ。

SSLとSETでは、誰がそのデータを復号化するかが異なっている。SSLでは、暗号化されたクレジットカード番号などは、受け取ったウェブサイトのサーバー自身が復号化していた。しかしSETでは、カード発行会社のサーバーで復号化される。ショッピングサイトには、カード発行会社から、クレジットカード番号ではなくカード発行会社が発行したSETだけで使える会員番号が送られる。つまりカード番号はカード会社にだけ渡り、ショッピングサイトにはカード番号が渡らないので、さらに安全であるというわけだ（図参照）。

ただ、SETでは、データがいくつかの中間ルート（加盟店、認証機関、加盟店管理会社）を経て、会員から発行会社まで流れるため、中間ルートそれぞれでの復号化やデータ盗難の防止を図る必要がある。そのための規格作りや動作確認の実証実験はスタートしたばかりで、現在はまだどこでも利用できるというわけではないが、より安全な決済方法が、誰でも、どこでも使えるようになるのは遠いことではないだろう。